(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 March 2003 (06.03.2003)

PCT

(10) International Publication Number
WO 03/019856 A2

(51) International Patent Classification[7]: H04L 9/32, H04Q 7/38, H04L 29/06

(21) International Application Number: PCT/CA02/01352

(22) International Filing Date: 30 August 2002 (30.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,356,420 30 August 2001 (30.08.2001) CA

(71) Applicant *(for all designated States except US)*: **WMODE INC.** [CA/CA]; 3553 - 31st Street N.W., Calgary, Alberta T2L 2K7 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MULLEN, Thomas, J.** [CA/CA]; 43 Oakmount Court S.W., Calgary, Alberta T2V 5B9 (CA). **SHARMAN, Duane** [CA/CA]; 955 Lake Placid Drive S.E., Calgary, Alberta T2J 4Z9 (CA).

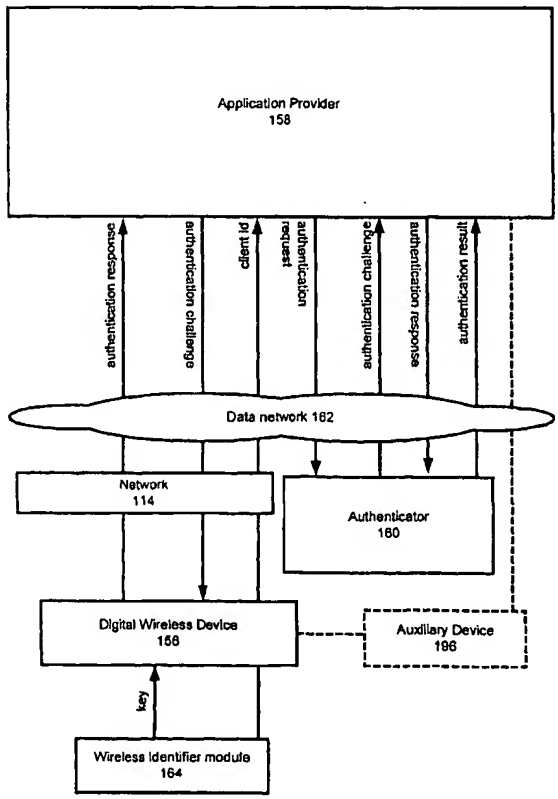
(74) Agents: **KINSMAN, Leslie, Anne** et al.; Borden Ladner Gervais LLP, World Exchange Plaza, 100 Queen Street, Suite 1100, Ottawa, Ontario K1P 1J9 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Continued on next page]

(54) Title: AUTHENTICATION AND NON-REPUDIATION OF A SUBSCRIBER ON A PUBLIC NETWORK



(57) Abstract: A system and method for authenticating a subscriber to an application provider using the authentication services of the wireless network over which the connection is made. A unique client id is provided, over a public network, by a wireless device to an authenticator. An authentication challenge is returned to the wireless device, which generates a response in accordance with a shared secret key. The response is transmitted back to the authenticator, which, if it determines the response to be authentic, permits the wireless device to connect to the desired application provider. A method and system for obtaining non-repudiable authorization for a billing transaction, so that charges can be placed on a network access billing system by an outside service provider, is also disclosed.

WO 03/019856 A2

ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AUTHENTICATION AND NON-REPUDIATION OF A SUBSCRIBER ON A PUBLIC NETWORK

FIELD OF THE INVENTION

The present invention relates to authenticating a subscriber on a public network. In particular, the present invention relates to a system for authenticating the identity of a user using a mobile device, such as a cellular phone, to log in to an application provider.

BACKGROUND OF THE INVENTION

In the field of wireless telecommunications, authentication of a user's identity is of fundamental concern. Three of the most substantial concerns regarding identity relate to whether or not the wireless device is legitimately identifying itself instead of reporting a false identification sequence, whether or not the handset is in the possession of the authorized user and generating an audit trail for billing purposes.

To facilitate the solution to the second problem, and to allow user billing, each wireless device is assigned a unique wireless device identifier, which is reported to the network upon initialization of the phone. The cellular phone service provider can check this wireless device identifier to ensure that the wireless device has not been reported stolen. Thus the assumption is made that unless reported stolen, a phone is in the hands of an authorized user, and that until reporting the phone missing the user is responsible for all charges incurred.

In traditional analogue cellular service, such as advanced mobile phone system (AMPS), narrowband AMPS (NAMPS), total access communications system (TACS), or extended TACS (ETACS) networks, though the wireless device identifier may be useable for identifying a stolen phone, it cannot be used to determine that the phone transmitting the ESN is doing so legitimately. The transmission of the wireless device identifier over an insecure network allows a third party to intercept the wireless device identifier. Because no information, other than the wireless device identifier, is required to validate a phone, a sufficiently motivated and properly equipped third party can scan known cellular channels to obtain wireless device identifier as phones are initialized. By modifying a second phone

to transmit the wireless device identifier of a first phone, it is possible to produce a cloned phone capable of convincing the network that it is authorized.

Along with offering encryption for phone calls to impede eavesdropping, digital cellular service also introduces a more secure initialization routine to make phone cloning more difficult. Due to its worldwide use, and simple to describe implementation global system for mobile communications (GSM) type systems will be used in the following discussion. It will be appreciated by one of skill in the art that the discussion is equally applicable to other communication systems such as time division multiple access (TDMA) and code division multiple access (CDMA). In digital service initialization, as illustrated in Figure 1, the wireless device identifier, such as an electronic serial number (ESN), is provided by the digital wireless device **112** to the digital cellular network **114**, as shown in flow **116**. The ESN is verified by checking against a database, such as an equipment identity register (EIR), in step **118**, and is rejected at **120** if it is determined to be an invalid ESN. If the ESN is valid, an authenticator **122**, such as an authentication center (AuC), transmits an authentication challenge in step **124**. Associated with each unique ESN is a predetermined secret key value, that is only stored in the cellular device **112** and AuC **122** and that is used to calculate a response such as a signed response (SRES) **126**. This secret key value is commonly referred to as the shared secret key. The SRES is transmitted **130** by the cellular device to the AuC **122**, which also calculates an SRES **128**. The two SRESs are compared in step **132**, and only upon matching is authentication of the digital wireless device provided **134**.

The authentication challenge can be used, in conjunction with the shared secret key value, to generate an SRES in numerous manners, including polynomial expansions of the values, and encrypting the shared secret key using the seed value as the public encryption key. Thus, by adding a securely stored value, the shared secret key, that is associated with a unique value, the ESN, and never openly transmitting the securely stored value, digital cellular services have a method of preventing one cellular device from impersonating another. In order to clone a first digital cellular phone **112**, a second digital wireless device would need to be reprogrammed to transmit the ESN of the first device and have the shared secret key value copied as well. Typically, the shared secret key value can only be

discerned by physical examination of the first digital wireless device **112**, or the AuC **122** of the digital cellular network **114**. After receiving authentication, digital cellular devices use a mix of encryption, spread spectrum transmissions and pseudo-random frequency hopping to provide second transmission channels.

Another advance digital cellular service offers over an analogue service is the ability to use the cellular device for more than audio signals. With analogue service, a computer could be connected to a modem, which in turn would connect to the analogue cellular device to provide a dial-up data connection. These connections are typically slow, noisy and insecure. In contrast, digital cellular services are by nature better designed to handle digital communications. Voice calls on a digital cellular network are packetized prior to transmission, and are transmitted as a series of binary representative packets. This allows digital cellular devices to interact with computers without the need for a modem. It also allows digital cellular devices to serve as digital wireless data stations.

So called wireless web functionality, wherein cellular devices allow a user to browse a subset of internet web sites through a proxy server or directly if the web site offers wireless markup language (WML) services, are already commonly implemented. Numerous services, from stock pricing to sports scores are commonly offered by application providers (AP), such as wireless application service providers (WASP). Additionally interactive services, such as banking transactions and stock trading can also be offered to users. These services are typically accessed through a data network that relies upon the transmission of data as packets. In many implementations the data is transmitted in packets conforming to the standards of the transmission control protocol/internet protocol (TCP/IP) suite. To translate between the wireless protocols of the network **114** and the wired protocols of data networks, such as the Internet, a gateway, such as a wireless application protocol (WAP) gateway, may be employed. This does not allow a connection from a digital wireless device **112** to a WASP that is guaranteed to be carried in a secure channel. One remedy is the use of a secure, or encrypted, connection between the WASP and the WAP gateway.

These wireless application service providers typically require a combination of user identifier and password to identify the user and select the corresponding account

information. Though transmitted over a semi-secure connection, many people's user identification and password information are easy to discern. Due to the limited interface of the majority of digital cellular devices many user identification and password combinations are very short, and thus more readily fall prey to conventional social engineering techniques, thus making illicit access to wireless ASP services easier to access than typical non-wireless systems.

By discerning user identification and password information, it is possible to impersonate a user of a WASP from any digital cellular device. Additionally the impersonation requires less effort than the cloning of an analogue cellular phone does, as impersonation requires no specialized equipment, whereas cloning analogue cellular devices requires equipment to reprogram electrically erasable programmable read only memory (EEPROM).

The client id can also be falsified by a computer with access to the WASP over a network. The data sent, in reply, by the WASP, is directed to the address of the computer that transmitted the packet, and not to a specific digital cellular phone. Thus an individual could falsify a client ID field and attempt to interact with the WASP, using discerned user identification and password information, without the WASP knowing that an unauthorized access had been performed.

Because it is not possible for a WASP to ensure that the user using the service is the authorized user, it is difficult to authenticate a user request in a manner that prevents the user from repudiating the transaction at a later time. Due to the ability of the user to repudiate transactions, forming fee per use billing arrangements with cellular service providers is difficult. Though banking institutions are content to carry out their own authentication and billing, other financial services, or services associated with personal information, lack the infrastructure to either bill a client on a fee-per-transaction basis or obtain a non-repudiable transaction authorization. One such example is a gaming service that allows wireless online gaming and requires the ability to bill small amounts of money to a carrier billing system per session. Another example is a stock monitoring service, where a user does not carry out a transaction, but does require authentication of the user to

protect the privacy of a user's portfolio, that would benefit from the ability to offer the same levels of security as the basic network requires.

Currently, digital wireless devices support WML through integrated WAP browsers, and included in this dialect is a "sign text" function that can be used to digitally sign requests. This function is embedded in the hardware of the phone and operates in the following manner:

a) WML script which contains sign text command is loaded into wireless device from web site;

b) Sign text function presents the specified text string to the subscriber on the phone;

c) Subscriber must enter a PIN known to subscriber and phone to sign the document; and

d) Upon entering the PIN the text is passed to the SIM and 'digitally signed" using a public key infrastructure (PKI) key pair specified in the sign text command.

Implementing this system requires that a PKI infrastructure be implemented by the WASP, and that the implemented PKI infrastructure is approved by the network **114** so that transactions can be approved, and if needed bill by the network **114**. Implementing a PKI infrastructure for every WASP and carrier is logistically difficult.

It is therefore desirable to provide a system and method for remote authentication of a wireless device for a service, without requiring the cumbersome step of requiring a user identification and password entry on the form factor limited input device. It is further desirable to provide a method of authorizing a WASP to bill a user through the wireless cellular provider, with proof that the WASP received authorization for the billing.

SUMMARY OF THE INVENTION

It is an object of the present invention to obviate or mitigate at least one disadvantage of the prior art.

In a first aspect, the present invention provides a method for providing authentication of both a digital wireless device having both a client identifier and a shared secret key, by an application provider connected to an authenticator where copies of both the client identifier

and shared secret key are held, and the channel between the application provider and the digital wireless device. The method of the first aspect of the present invention comprises the authenticator receiving a request to authenticate a digital wireless device from the application provider, said request optionally including the client identifier of the digital wireless device to be authenticated, the authenticator generating an authentication challenge in response to the received request and then transmitting the challenge to the digital wireless device, whereupon the digital wireless device generates and transmits a response to the authentication challenge, said response optionally being generated by use of the shared secret key, which upon being received by the authenticator is authenticated, the authentication results being provided to the application provider. In an embodiment of the first aspect of the present invention communication between the application provider and the authenticator is carried by a data packet protocol, such as one provided in the transmission control protocol/internet protocol suite, and is carried over a network such as the Internet. In another embodiment, communication between the authenticator and the digital wireless device is carried out using the application provider as an intermediary, while communication between the application provider and the digital wireless device is carried out using a digital wireless network, such as a digital cellular network employing time division multiple access, code division multiple access, the global system for mobile communications, or other such digital cellular protocols, as an intermediary.

According to a further aspect of the present invention, there is provided a system for authenticating a digital wireless device, having both a client identifier and a shared secret key, for an application provider, connected to a data network, that is in communication with the digital wireless device comprising an authenticator, which optionally holds the key associated with the client id of the digital wireless device, that is operatively connected to the application provider over the data network for receiving requests from the application provider to authenticate the digital wireless device, for generating and transmitting authentication challenges, receiving and authenticating responses to the authentication challenges and for transmitting to the application provider the result of the authentication of the received responses. In an embodiment of the present aspect the data network is a network such as the Internet that is based on a protocol such one included in the transmission control

protocol/internet protocol suite. In another embodiment of the present invention the digital wireless device is connected to the application provider by a digital wireless network, said digital wireless network being optionally connected to the application provider by the data network.

In another embodiment, there exists an auxiliary device connected to the digital wireless device, optionally over a wireless connection, and the application provider, optionally over the data network, for transmitting to the application provider the client id of the digital wireless device, and for acting as an intermediary between the application provider and the digital wireless device wherein it receives from the application provider authentication challenges for the digital wireless device, provides the received authentication challenges to the digital wireless device, receives from the digital wireless device responses to the received challenges and provides the received responses to the application provider. In this embodiment the authentication of the channel covers the channel between the application provider and the digital wireless device through the auxiliary device.

In a presently preferred embodiment, there is provided a system, as described above, wherein the digital wireless device is operatively connected to the application provider for receiving a transaction request, and has digital signature means for signing the transaction request and transmission means for transmitting the signed transaction request to the application provider, furthermore the authenticator includes means for receiving the signed transaction request, authenticating the signed transaction request, said means optionally using a copy of the initial transaction request and a value derived from the client id, and transmission means for transmitting the results of the authentication of the signed transaction request to the application provider.

In a further aspect, there is provided a method of obtaining non-repudiable authorization, for a transaction, from a digital wireless device having both a client identifier and a shared secret key, at an application provider connected to both an authenticator knowing the shared secret key associated with the client identifier of the digital wireless device, and the digital wireless device, the method comprising the steps of the application provider transmitting a transaction request to the digital wireless device, the digital wireless device digitally signing the transaction request, which optionally includes the step of encrypting the

transaction request with the shared secret key, and transmitting the digitally signed transaction request to the application provider, and the authenticator authenticating the digitally signed transaction request optionally using a copy of the transaction request and the shared secret key associated with the client id of the digital wireless device.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the attached Figures, wherein:

Figure 1 is an illustration of the prior art authentication process for a digital cellular network;

Figure 2 is an illustration of a system of the present invention to facilitate authentication of a user device by an application provider;

Figure 3 is a flowchart of an authentication process of the present invention;

Figure 4 is an illustration of a system of the present invention to facilitate authentication of a digital wireless device's digital signature on a transaction request from the application provider;

Figure 5 is a flowchart of a method of the present invention to provide a non-repudiable transaction authorization from the user device; and

Figure 6 is an illustration of a system of the present invention to provide authentication and transaction services for an application provider to authenticate the user of an auxiliary device using the authentication features of a digital wireless device.

DETAILED DESCRIPTION OF THE INVENTION

The present invention will be described in relation to the Figures. One of skill in the art will appreciate that a number of changes can be made to the presented system and method to accomplish the same object without departing from the scope of the present invention.

Figure 2 presents a system according to an embodiment of the present invention. Digital wireless device **156**, in a present embodiment a digital wireless device such as a cellular phone, is connected to network **114**, which provides a connection to an application

provider (AP) **158**, which in a present embodiment is a wireless application service provider, through data network **162**. The connection between network **114** and data network **162** may be through a gateway or translation device as will be appreciated by one of skill in the art. In the presently illustrated embodiment, all communication between the digital wireless device **156** and the network **114** is carried out using standard radio frequency (RF) protocols. All communication between the application provider **158** and other components is carried out using standard data transfer protocols such as those in the transmission control protocol/internet protocol (TCP/IP) suite.

Upon connecting to the AP **158**, through network **114**, a client id uniquely associated with digital wireless device **156** is provided to AP **158**. The client id can originate in the digital wireless device **156**, or digital identifier module **164**. Alternatively, network **114**, using a standard gateway such as a wireless application protocol gateway, can attach the client id to data transmissions originating from digital wireless device **156**. Digital identifier module **164** is, in one embodiment, a subscriber identification module (SIM) that is removable from the digital wireless device **154**. In other embodiments, the digital identifier module **164** is integrated with the digital wireless device **154**, so as not to be removable, and can encompass any means of storing the client id and shared secret key in the wireless device **154**. Authenticator **160** is connected to AP **158** through data network **162**. Data network **162** is a packet-based network such as the Internet.

Optionally included in the system of Figure 2 is auxiliary device **196**, which is directly connected to digital wireless device **156**, and connected to AP **158** through data network **162**.

A method according to the present invention is shown in Figure 3, with the data flows shown in Figure 2. Generally, AP **158** associates the unique client id with its own account information. To ensure that a malicious third party does not forge a client id, AP **158** confirms that the source of the client id is a valid party. The process commences when the AP **158** receives a connection request from the digital wireless device **156** at step **166**. This request includes the client id of the digital wireless device **156** that is initiating the connection, or in an alternate embodiment the request can include any value uniquely associated with the client id, such as the ESN or phone number of the digital wireless

device. The authenticator **160** is asked to authenticate the user in step **168**. The authenticator **160** then generates an authentication challenge based upon the client id, or other value associated with the client id, step **169**. This authentication challenge is similar to the one that would be generated when a digital wireless device is initialized on the network **114**. The authenticator then transmits the generated challenge to the AP **158** at step **170**. AP **158** then transmits the authentication challenge to the party that initiated the connection at step **171** (whose network address is determined from the incoming request). If the request is from digital wireless device **156**, it receives the authentication challenge, and calculates an authentication response.

The digital wireless device **156** receives the authentication challenge from AP **158** and responds by generating an authentication response in step **172**. The authentication response is calculated using a shared secret key stored in the wireless identification module **164**. The generated response is transmitted to the AP **158** in step **173**. The authentication response is transmitted by AP **158** to the authenticator **160** in step **174**. The authenticator **160** authenticates the provided authentication response in step **176**. Upon authenticating the authentication response, authenticator **160** provides AP **158** with the result of the authentication. If the authenticator **160** authenticated the authentication response successfully, the connection to the digital wireless device **156** is allowed to proceed and the account is accessed, as shown at step **178**. If the authentication response is not successfully authenticated the connection is rejected at step **180**.

In another embodiment of the method of the present invention, AP **158** requests authentication of a client id by interacting with authenticator **160**, and includes in the request the network address of digital wireless device **156**. Authenticator **160** transmits an authentication request to AP **158**. AP **158** relays the authentication challenge to digital wireless device **156**, which generates the authentication response and transmits it directly to authenticator **160**. Upon authenticating the authentication response, authenticator **160** provides AP **158** with the authentication result, which is used to determine whether or not to provide a connection with digital wireless device **156**. Thus authenticator **160** delivers a challenge to the originator of the connection to AP **158** to authenticate both digital wireless device **158**, and the connection between digital wireless device **156** and AP **160**.

As will be appreciated by those of skill in the art, by providing a connection between the AP **158** and the authenticator **160**, it is possible to authenticate digital wireless device **156** without requesting that user information be input by the user. This provides the same degree of authentication that network **114** provides for basic network service. Thus possession of the digital wireless device **156** is considered to be permission to access the services of AP **158**, and the onus to report a device theft is placed upon user.

An example of a user being authenticated using the method of Figure 3 and the system of Figure 2 is now provided, for illustrative purposes only. This example should not be construed as limiting to the scope of the present invention. A user controls the digital wireless device **156**, and creates a connection, over network **114**, to a stock quote service's AP **158** with which a series of accounts have been established, each account holding a number of stocks that are tracked. The AP **158** receives a request for a connection, which includes a client id. Seeking to authenticate that the client reported is from the device registered by the user, AP **158** connects to the authenticator **160** and requests an authentication of the client id reported by the incoming connection to AP **158**. Authenticator **160** then generates an authentication challenge. The challenge is provided to the AP **158**, which then transmits the challenge to digital wireless device **156**. The digital wireless device **156** calculates an authentication response that will identify it to the authenticator **160**, using the shared secret key associated with its client id. The authentication response is provided to the authenticator **160** by AP **158** upon receiving it from digital wireless device **156**. The authenticator **160** then verifies that a party that knows the shared secret key generated the authentication response. This information is considered to be proof that the digital wireless device **156** is valid and not cloned, nor is the connection request from a source attempting to masquerade as digital wireless device **156**. Upon receiving the result of the comparison between the provided authentication response and the authenticator calculated authentication response, AP **158** accepts the connection if the comparison revealed that the authentication response was valid. The client id of the incoming connection is then used, by the AP **158** to identify the user, and present the relevant information about the stocks in each account. The matching of the client id and user information is done in a database hosted by AP **158**.

Because the authentication of a user is as secure as that offered for basic network service, it is possible for an infrastructure to be built that allows the AP **158** to bill through the network billing system as, with the above mentioned system, user authentication is now sufficiently secure. A system, to do implement AP **158** to network **114** billing, a method of obtaining non-repudiable user permission for billing must be implemented. A method of obtaining non-repudiable transactions has other addition uses such as providing proof of approval for account status changes. Such a figure is illustrated in Figure 4. Figure 4 maintains the same network topology as the system of Figure 2, but illustrates different data flows. Despite the fact that the user device **112** has been authenticated, AP must still obtain proof that the user has authorized a transaction. This approval can be assumed if AP **158** is considered to be a trusted party by network **114**, typically this would require a standing relationship. Alternatively the AP **158** can issue a transaction request to digital wireless device **156** to approve a transaction, and provide a digitally signed response as proof of approval. This transaction request is provided to digital wireless device **156** through the network **114**, after being generated by AP **158**. The transaction response containing the approval for billing is generated by digital wireless device **156** by encrypting and/or hashing the transaction request with the shared secret key, or a value derived therefrom. Approval of the transaction is provided by digital wireless device **156**, and is transmitted through network **114** to AP **158**. The transaction response, and a copy of the transaction request, along with the client id are then provided to authenticator **160**. Using the shared secret key, associated with the client id, it is possible for the authenticator to authenticate that digital wireless device **156** signed the transaction request. The result of the transaction authentication is then provided to the application provider.

A flowchart, demonstrating a further steps to provide subscriber non-repudiation according to the method of the present invention is illustrated in Figure 5, with the data flows illustrated in Figure 4. Upon receiving authentication of the digital wireless device **156**, from the authenticator **160**, the AP **158** allows a connection to be established with digital wireless device **156** in step **182**. At a certain point in the connection, AP **158** determines that it requires authentication of a transaction from digital wireless device **156**. The authenticated transaction, which is non-repudiable, could be instructions to bill for a

service provided, instructions to carry out a financial transaction, or any service for which the AP desires proof that the instructions are from digital wireless device **156**. AP **158** then transmits a transaction request to digital wireless device **156** in step **184**. Typically, the transaction request is a text message from AP **158** that is displayed by the user device. The user digitally signs the request in step **186** by selecting a prompt, inputting an identification number, or other method that will be apparent to one of skill in the art. In order to provide AP **158** with non-repudiation, the request is signed by hashing and/or otherwise encrypting the request with either the shared secret key used in the generation of the authentication response or a value derived therefrom. One of skill in the art will appreciate that a number of known techniques could be applied to provide non-repudiation using either the authentication response or the shared secret key, or a combination of the two, without departing from the spirit of the present invention. In a presently preferred embodiment, the user of digital wireless device **156** must input a personal identification number that is known to both the user and digital wireless device **156** in order to digitally sign the request, in an alternate embodiment the user must simply respond by selecting a transaction confirmation option. In step **188**, AP **158** transmits the transaction request, the transaction response, and the client id of digital wireless device **156** to the authenticator **160**. The authenticator **160**, using the shared secret key associated with the provided client id, authenticates the digitally signed document. In a presently preferred embodiment the authentication of the document is provided by encrypting and/or hashing the transaction request, as done in digital wireless device **156**, with the shared secret key, and comparing the result to the provided transaction response, providing AP **158** with a non-repudiable authorization to carryout the approved transaction. In an alternate embodiment, the encrypting of the transaction request is preformed using both a value derived from the shared secret key, and a value derived from the current time. This allows the authenticator to ensure that a given transaction request is authenticated within a fixed time interval to prevent an AP from re-submitting a request multiple times. Upon authenticating the digitally signed request the authenticator **160** transmits the authentication results to the AP **158**, which uses the results for a decision in step **190**. If the authentication of the digitally signed transaction has failed, the transaction is rejected in step **192**. If the authentication of

the digitally signed transaction is successful the AP proceeds with the transaction in step **194**.

An further embodiment of the system of the present invention is illustrated in Figure 6. AP **158** is connected to authenticator **160** as previously described. Additionally an auxiliary device **196**, such as a personal computer, is connected both AP **158**, through a data network, and the digital wireless device **156**. A user controls both digital wireless device **156** and auxiliary device **196**. The connection between digital wireless device **156** and auxiliary device **196**, may be wireless, by means of a dial-in connection, a Bluetooth™ wireless link, an infrared connection, or other means known to one of skill in the art, or it could be a wired connection from a data port on digital wireless device **156** to an input on auxiliary device **196**. The auxiliary device **196** is connected to AP **158**, through a data network, and serves as the primary method of interacting with AP **158**. The manner of connection between auxiliary device **196** and AP **158** does not necessarily have to be either wireless, or permanent. The requests for authentication and approval for billing that were previously transmitted to the digital wireless device **156** over network **114**, are instead transmitted from AP **158** to the auxiliary device **196** over a data network. The auxiliary device **196** then transmits the received requests to the digital wireless device **112**, and forwards all responses to AP **158**.

The system of Figure 6, allows an auxiliary device **196** to be authenticated in the same manner as the digital wireless device **156**, without digital wireless device **156** needing to directly access network **114**. In operation auxiliary device **196** provides a client id, or a value associated with the client id, to AP **158**. This client id, can by manually input by the user or obtained from a connection to digital wireless device **156**. AP then submits an authentication request to authenticator **160** over data network. Authenticator **160** provides an authentication challenge, based upon the client id, to the auxiliary device, via AP **158**. Auxiliary device **196** provides the authentication challenge to digital wireless device **156**, which uses the shared secret key in the wireless identification module, or a value derived therefrom, to calculate an authentication response, which is provided to auxiliary device **196**. Auxiliary device **196** transmits the authentication response to authenticator **160** via AP **158**. Authenticator **160** authenticates the provided authentication

response and provides the authentication result to AP **158**, which can optionally share the authentication result with auxiliary device **196**.

For exemplary purposes the system of Figure 6, and elements of the figure, will be used to provide a description of a system that uses the authentication and transaction authentication processes outlined above, to complete a transaction. It is increasingly common for a user, to have digital wireless device **156** present at all times. Thus it may be desirable to use digital wireless device **156** as a method of payment for various goods and services. Auxiliary device **196** is , for the purposes of this example, a vending machine. Upon making a selection from the machine, either using a wireless connection from digital wireless device **156** or by manually interacting with vending machine **196**, the user elects to pay for the products through a charge on the account associated with digital wireless device **156**. The vending machine **196** communicates with a centralized AP **158** that serves to track billing transactions. The centralized AP **158** needs to authenticate the digital wireless device **112** that will be paying for the transaction and then needs to obtain approval for the transaction. Vending machine **196** communicates with digital wireless device **156** by means of a wireless connection, such as a Bluetooth™ connection. The digital wireless device **156** then provides to the vending machine **196** a client id, which is provided to the authenticator **160** by AP **158**. The authenticator **160** generates an authentication challenge for the digital wireless device **156**, as described above. The challenge is provided to the digital wireless device through AP **158** and the vending machine **196**. The digital wireless device **156** responds with an authentication response that is provided to the authenticator **160** through the vending machine **196** and the AP **158**. The authentication is confirmed and AP **158** transmits a request to approve the billing transaction to the digital wireless device **156** through the wireless Bluetooth™ connection between the digital wireless device **156** and the vending machine **196**. The request to approve the billing transaction is approved by the user, and digital wireless device **156** creates a reply that is comprised of the request to approve billing modified by the shared secret key associated with the client id. This information is provided to the authenticator **160** via AP **158** and vending machine **196**. Authenticator **160** then authenticates the transaction request and provides an authentication request to AP **158**. AP **158** then bills the

user's account in the billing system of network **114** (not shown). Upon transmitting a billing transaction to the billing system, AP **158** instructs the vending machine **196** to dispense the products that were paid for.

In an alternate embodiment of the present invention, the auxiliary device **196** is a personal computer (PC), connecting over a data network **162**, such as the internet to AP **158**. PC **196** is controlled by a user, and connects to AP **158** to carry out a transaction. AP **158** receives the connection, and is provided with the client id associated with digital wireless device **156**, or another value that is uniquely associated with the client id such as the phone number of digital wireless device **156**. AP **158** needs to authenticate the identity of the connecting device, so requests authentication from authenticator **160**. Included in the authentication request is the identifying information that is uniquely associated with the client id of digital wireless device **156**. Authenticator, using the identifying information generates an authentication challenge based upon the shared secret key associated with the identifying information, and provides the authentication challenge to AP **158**, which relays the challenge to PC **196**. PC **196** provides the authentication challenge to digital wireless device **156** over a wireless connection, such as a BlueTooth™ connection. Digital wireless device **156**, using the shared secret key held in wireless identifier module **164**, generates an authentication response which is provided to auxiliary device **196**, and relayed to authenticator **160** through AP **158** and data network **162**. Authenticator **160** authenticates the response and provides the authentication result to AP **158**, which can then provide service to PC **196**. Transaction requests can be signed in a similar manner as they were previously, using the channel illustrated here. Thus any auxiliary device that can communicate with digital wireless device **156**, can be authenticated by AP **158** by authenticator **160**.

Because there are a plurality of application providers that are not associated with each other, and a plurality of wireless networks, each of which have a distinct authenticator, it is foreseeable that a clearinghouse be implemented. Thus each AP can connect to the clearinghouse, and through the clearinghouse, have access to the authenticators of different networks.

The above-described invention provides the ability for an application provider to authenticate the identity of a subscriber with the same security and accuracy as a wireless network service provider has. This authentication of identity allows for easier logins to application providers, and provides additional security for a user by restricting access to a limited number of predetermined wireless devices. Additionally the above described invention provides a method of non-repudiable authorization for transactions that among other uses allows application providers to charge on a fee for service basis, and apply the charges to an account associated with the digital wireless device managed by the wireless network.

To implement such a system, minor modifications to the WML browser of current digital wireless devices would be required to modify the included signtext function in the phone to support digitally signing transaction requests, with the carriers shared secret key in place of the PKI keys. Additionally, this invention could be implemented through the creation of a new WML command to support the generation of the authentication response based on the authentication challenge. This would allow AP **160** to send the challenge to digital wireless device **158** using WML. The WML processor in the browser generates the Authentication response and sends the reply to AP **160**.

The above-described embodiments of the invention are intended to be examples of the present invention. Alterations, modifications and variations may be effected to particular embodiments by those of skill in the art, without departing from the scope of the invention which is defined solely by the claims appended hereto.

What is claimed is:

1. A method of authenticating a digital wireless device having both a client identifier and a shared secret key, by an application provider connected to an authenticator where copies of both the client identifier and shared secret key are held, the method comprising the steps of:

receiving at the authenticator, a request to authenticate a digital wireless device from the application provider;

generating an authentication challenge at the authenticator;

transmitting the authentication challenge to the digital wireless device;

transmitting, from the digital wireless device, a response to the authentication challenge;

determining the authenticity of the response to the authentication challenge, at the authenticator; and

transmitting the determined authenticity of the response to the authentication challenge to the application provider.

2. The method, as in claim 1, wherein the authenticator communicates with the application provider using a data packet protocol.

3. The method, as in claim 2, wherein the data packet protocol is a part of the transmission control protocol/internet protocol suite.

4. The method, as in claim 3, wherein communication between the application provider and the authenticator is carried by the Internet.

5. The method, as in claim 1, further comprising the step of transmitting the authentication challenge to the application provider, after generating the authentication challenge at the authenticator.

6. The method, as in claim 5, wherein communication between the application provider and the digital wireless device is carried by a digital wireless network.

7. The method, as in claim 6, wherein the application provider and the digital wireless network communicate using a protocol that is part of the transmission control protocol/internet protocol suite.

8. The method, as in claim 6, wherein the digital wireless network and the digital wireless device communicate using a digital cellular protocol.

9. A method, as in claim 8, wherein the digital cellular protocol is time division multiple access.

10. A method, as in claim 8, wherein the digital cellular protocol is code division multiple access.

11. A method, as in claim 8, wherein the digital cellular protocol is global system for mobile communications.

12. The method, as in claim 1, wherein the response to the authentication challenge is transmitted from the digital wireless device to the application provider.

13. The method, as in claim 12, wherein the response to the authentication challenge is transmitted from the application provider to the authenticator after being received by the application provider, prior to determining the authenticity of the response.

14. The method, as in claim 1, wherein the request for authentication from the application provider includes the a value uniquely associated with the client identifier of the digital wireless device.

15. The method, as in claim 14, wherein the authentication challenge is generated to be specific to the client identifier of the digital wireless device.

16. The method, as in claim 15, wherein the response to the authentication challenge is calculated using the shared secret key associated with the client identifier of the digital wireless device.

17. A system for authenticating a digital wireless device, having both a client identifier and a shared secret key, for an application provider, connected to a data network, that is in communication with the digital wireless device, comprising:

an authenticator, operatively connected to the application provider over the data network, for receiving authentication requests for the digital wireless device from the application provider, for generating and transmitting authentication challenges, for receiving and authenticating authentication responses to generated challenges, and for transmitting to the application provider the result of the authentication of the received responses to the generated challenges.

18. The system, as in claim 17, wherein the data network is based on a protocol included in the transmission control protocol/internet protocol suite.

19. The system, as in claim 18, wherein the data network is the Internet.

20. The system, as in claim 17, wherein the digital wireless device and the application provider are connected by a digital wireless network.

21. The system, as in claim 20, wherein the digital wireless network and the application provider are connected by the data network.

22. The system, as in claim 17, wherein the authenticator holds the key associated with each client identifier.

23. The system, as in claim 17, wherein the application provider and authenticator are operatively connected by a clearinghouse.

24. The system, as in claim 17, further comprising an auxiliary device connected to the digital wireless device, and the application provider, for transmitting to the application provider the a value uniquely associated with the client identifier of the digital wireless device, receiving from the application provider authentication challenges, providing the received authentication challenges to the digital wireless device, receiving from the digital wireless device responses to the authentication challenges and providing to the application provider the received responses to the authentication challenges.

25. The system, as in claim 24, wherein the auxiliary device is connected to the application provider over the data network.

26. The system, as in claim 24, wherein the auxiliary device is connected to the digital wireless device over a wireless connection.

27. The system, as in claim 17, wherein the digital wireless device is operatively connected to the application provider for receiving a transaction request.

28. The system, as in claim 27, wherein the digital wireless device includes digital signature means for signing the transaction request and transmission means for transmitting the signed transaction request to the application provider

29. The system, as in claim 28, wherein authenticator includes means for receiving the signed transaction request, authenticating the signed transaction request and for transmitting the results of the authentication of the signed request to the application provider.

30. The system, as in claim 29, wherein the authenticator includes means for authenticating the digitally signed request using a copy of the initial transaction request and a value derived from the client identifier.

31. A method of obtaining non-repudiable authorization for a transaction, from a digital wireless device having both a client identifier and a shared secret key, at an application provider connected to both an authenticator having the shared secret key associated with the client identifier of the digital wireless device, and the digital wireless device, the method comprising the steps of:

transmitting, from the application provider, a transaction request to the digital wireless device;

digitally signing and transmitting the transaction request to the application provider; and

authenticating the digitally signed transaction request, at the authenticator.

32. A method, as in claim 31, wherein authentication of the digitally signed transaction request is performed using a copy of the transaction request and the shared secret key associated with the client identifier of the digital wireless device.

33. The method, as in claim 31, wherein the step of digitally signing includes the step of encrypting the transaction request with the shared secret key.

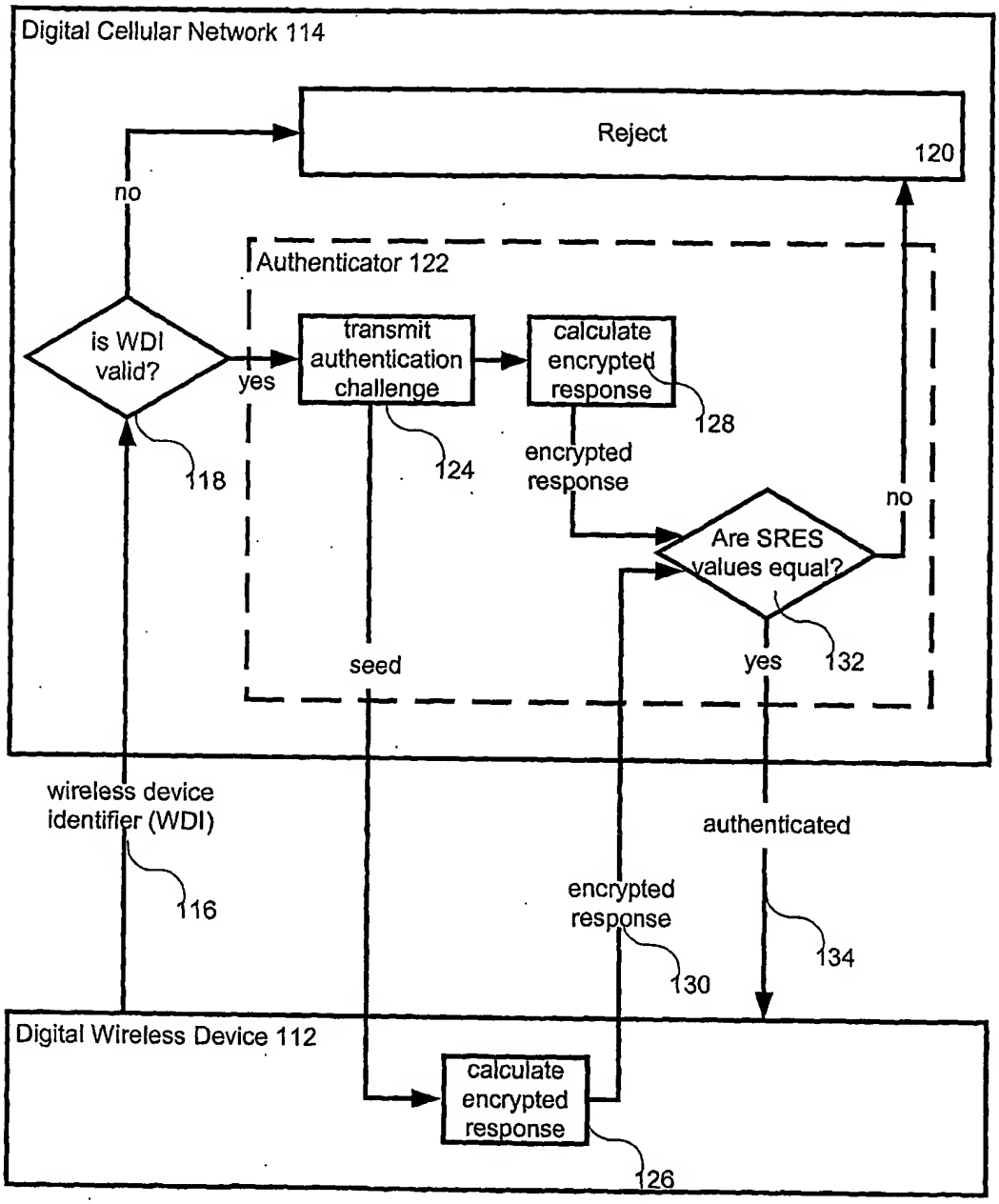


Figure 1 (prior art)

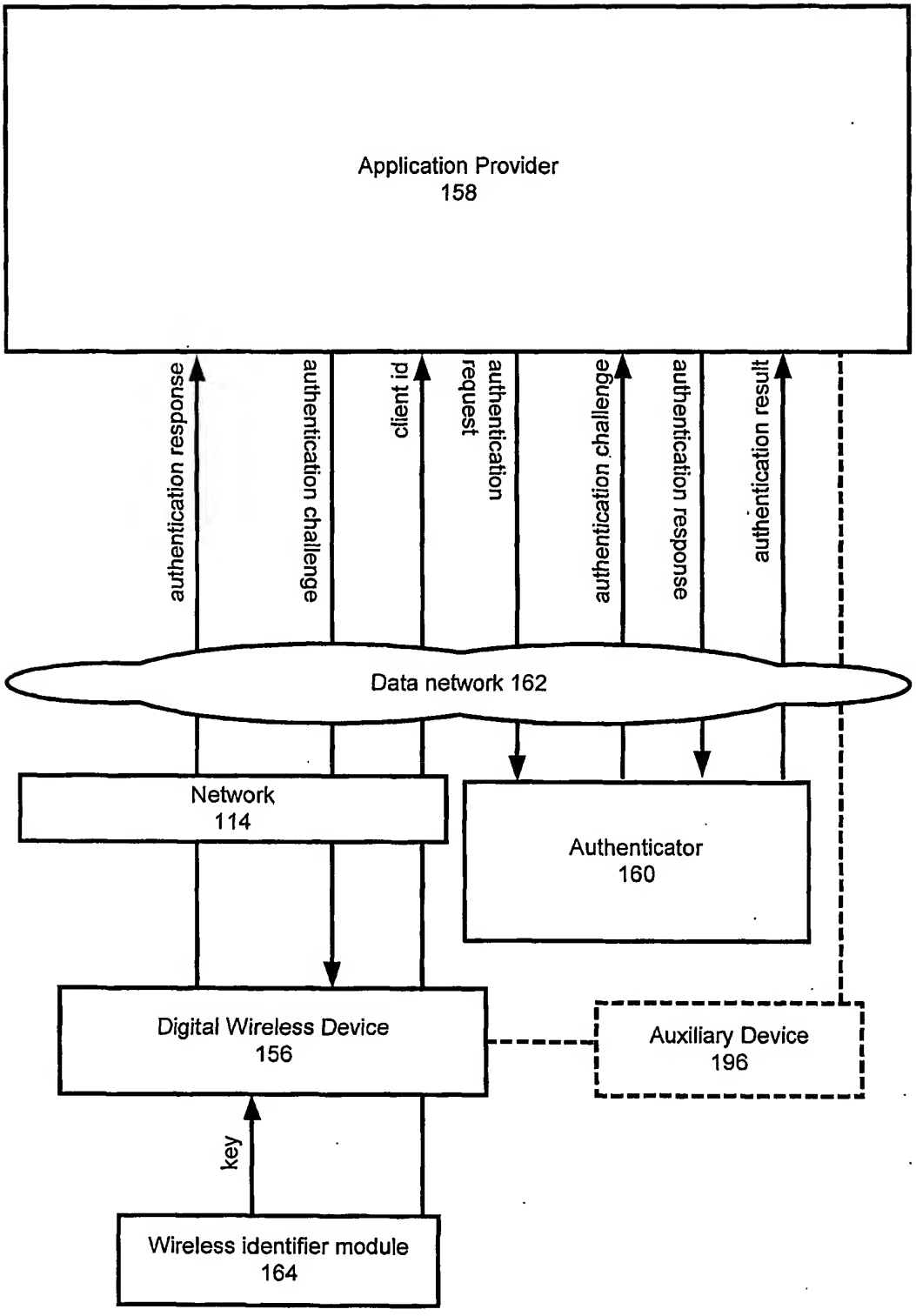

Application Provider
158
authentication response
authentication challenge
client id
authentication request
authentication challenge
authentication response
authentication result
Data network 162
Network
114
Authenticator
160
Digital Wireless Device
156
Auxiliary Device
196
key
Wireless identifier module
164

Figure 2

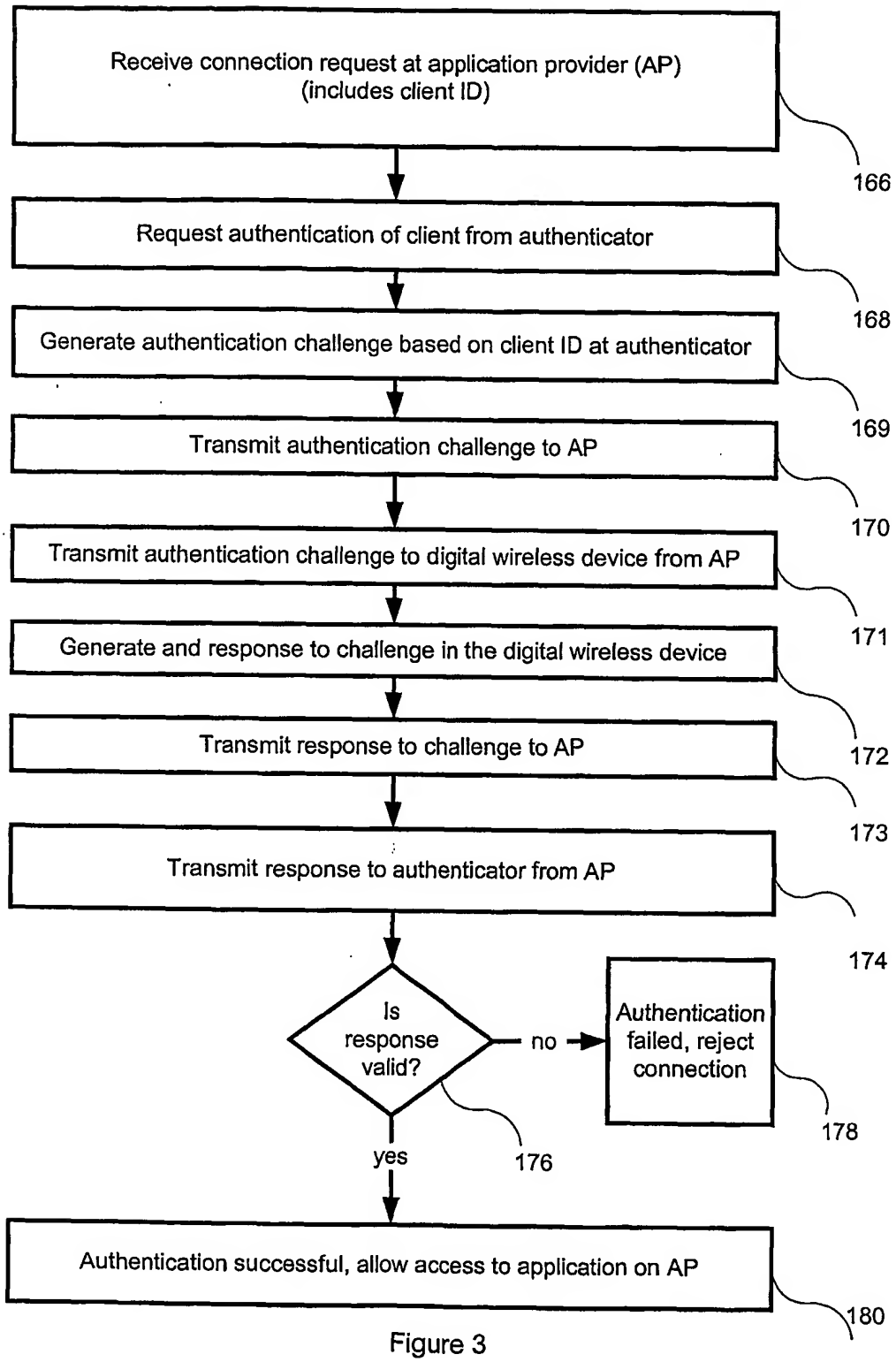

Receive connection request at application provider (AP) (includes client ID)
166
Request authentication of client from authenticator
168
Generate authentication challenge based on client ID at authenticator
169
Transmit authentication challenge to AP
170
Transmit authentication challenge to digital wireless device from AP
171
Generate and response to challenge in the digital wireless device
172
Transmit response to challenge to AP
173
Transmit response to authenticator from AP
174
Is response valid?
no
Authentication failed, reject connection
178
176
yes
Authentication successful, allow access to application on AP
180

Figure 3

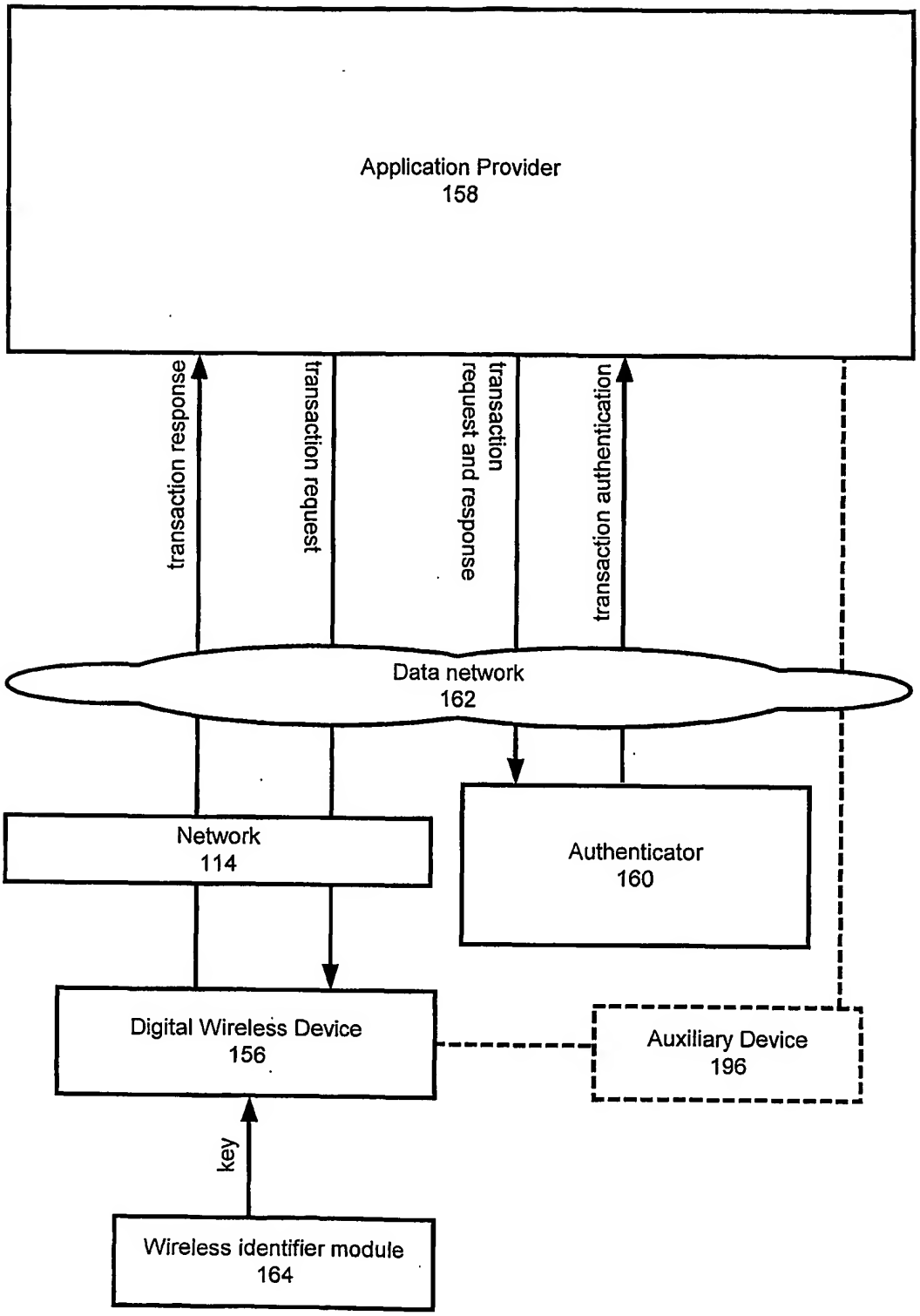

Application Provider
158
transaction response
transaction request
transaction request and response
transaction authentication
Data network
162
Network
114
Authenticator
160
Digital Wireless Device
156
Auxiliary Device
196
key
Wireless identifier module
164

Figure 4

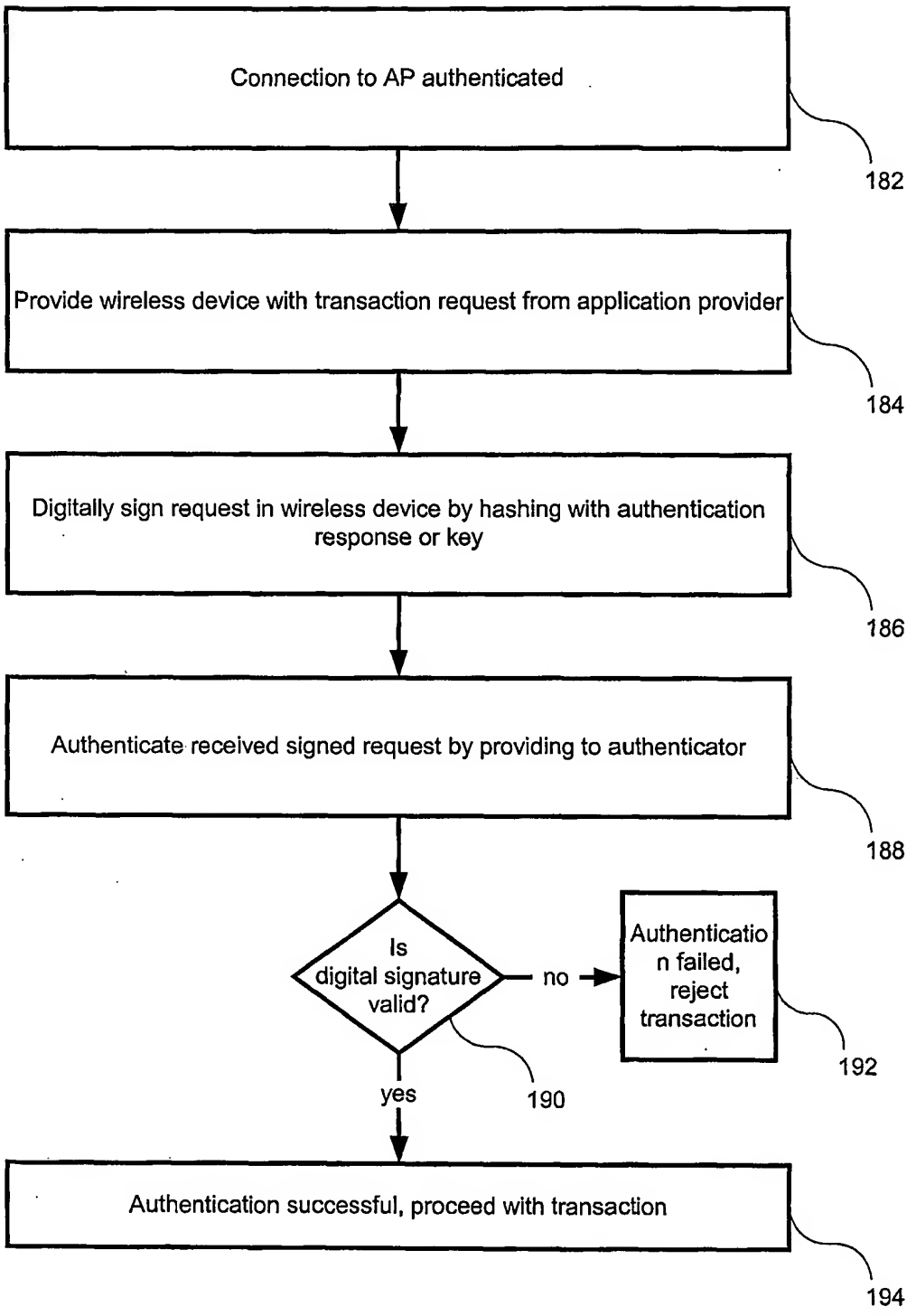

Connection to AP authenticated
182
Provide wireless device with transaction request from application provider
184
Digitally sign request in wireless device by hashing with authentication response or key
186
Authenticate received signed request by providing to authenticator
188
Is digital signature valid?
no
Authenticatio n failed, reject transaction
192
yes
190
Authentication successful, proceed with transaction
194

Figure 5

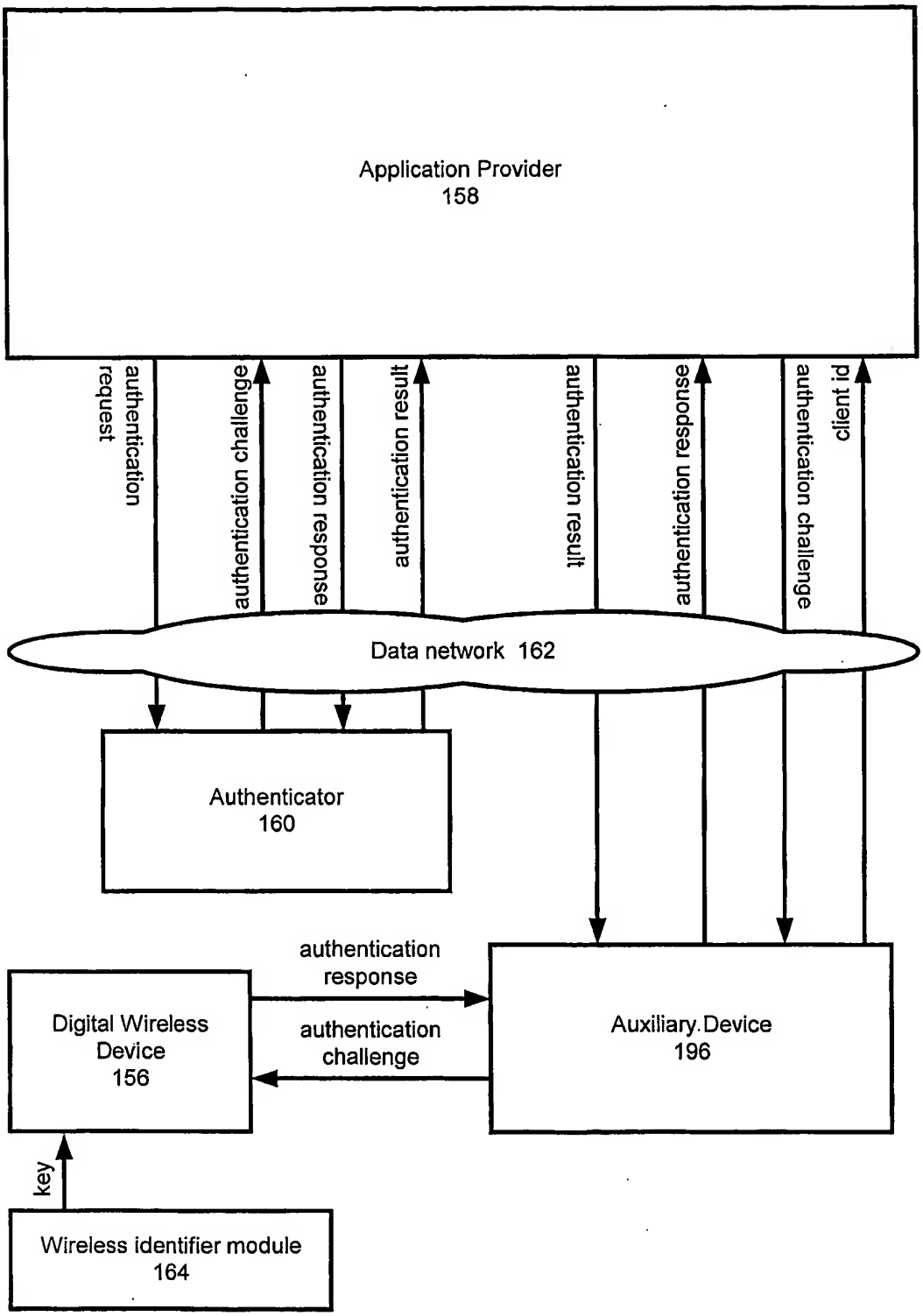

Application Provider
158
authentication request
authentication challenge
authentication response
authentication result
authentication result
authentication response
authentication challenge
client id
Data network 162
Authenticator
160
authentication response
authentication challenge
Digital Wireless Device
156
Auxiliary Device
196
key
Wireless identifier module
164

Figure 6